Claims

1. An authentication method of at least one client entity (A) by an authentication entity (B), said authentication entity (B) comprising a set of secret keys (K_{Ai}), each being associated with a client entity (Ai) capable of being identified by said authentication entity, said method being characterized in that it comprises the following steps consisting of:

a - transmitting an anonymous authentication request (Authentication Request) from the part of the client entity (A) to the authentication entity (B);

b - sending from the authentication entity (B) to the client entity, an authentication counter value (CB) corresponding to the current state of a counter (COMPTB) of the authentication entity (B);

c - verifying, at the client entity side (A), that the authentication counter value (CB) received is strictly greater than a counter value (CA) stored by the client entity (A);

d - calculating, at the client entity side (A), a counter signature by application of a cryptographic function (S) shared by the client entity (A) and the authentication entity (B), with said authentication counter value (CB) and a secret key (K_A) associated with the client entity (A) as operands;

e - transmitting said counter signature (S (K_A,CB)) to the authentication entity (B);

f - updating the counter value (CA) stored by the client entity (A) with said authentication counter value (CB);

g - searching, at the authentication entity side (B), for at least one client entity (A) capable of being identified, for which the corresponding counter signature (S (K_{Ai}, CB)) for said authentication counter value (CB) is coherent with the counter signature received (S (K_A, CB));

h - having the authentication counter (COMPTB) increase.

2. The authentication method according to Claim 1, characterized in that steps b) to h) are reiterated at least

once, so as to ensure that the client entity identified is identical at each iteration.

3. The method according to Claim 1 or 2, characterized in that the search step consists of:

i - calculating, for each client entity (Ai) capable of being identified, the corresponding counter signature (S (K_{Ai}, CB)) by application of the cryptographic function (S) with the authentication counter value (CB) and the secret key associated with (K_{Ai}) as operands, so as to compile a list of client entity capable of being identified/corresponding counter signature couples (Ai, S (K_{Ai}, CB)), for said counter value (CB);

j - verifying the coherence between the counter signature received (S (K_A, CB)) and at least one counter signature (S (K_{Ai}, CB)) of said list.

4. The authentication method according to Claim 3, characterized in that the list of client entity capable of being identified/corresponding counter signature couples (Ai, S (K_{Ai}, CB)) compiled for a given authentication counter value (CB), is ordered, at the authentication entity side, according to the value of said counter signature (S (K_{Ai}, CB)).

5. The authentication method according to Claim 3 or 4, characterized in that in the case of coherence between the counter signature received (S (K_A, CB)) and the counter signature (S (K_{Ai}, CB)) of a plurality of couples, steps b) to h) are reiterated until a single couple is obtained for which the counter signature corresponds to the counter signature received.

6. The authentication method according to Claim 5, characterized in that, during repetition of stage i), the counter signature (S (K_{Ai}, CB)) is calculated solely for the client entities (Ai) corresponding to said plurality of couples determined at the preceding iteration.

7. The authentication method according to any one of Claims 3 to 5, characterized in that it consists of implementing step i) as anticipated relative to an authentication request from a client entity (A) at step a), said anticipated step i) consisting of pre-establishing, at the authentication entity side (B), for at least one authentication counter value (CB) to come, the list of client entity capable of being identified/corresponding counter signature couples (Ai, S (K_{Ai}, CB)) for each of said authentication counter values to come, and storing said pre-established lists at the authentication entity side (B), any sending from the authentication entity (B) to the client entity (A) of an authentication counter value (CB), corresponding to sending an authentication counter value (CB) for which a list of client entity capable of being identified/corresponding counter signature couples (Ai, S (K_{Ai}, CB)) has already been pre-established.

8. The authentication method according to any one of the preceding claims, characterized in that step h) consists of increasing the authentication counter (COMPTB) by a fixed rate.

9. The authentication method according to any one of Claims 1 to 7, characterised in that step h) consists of increasing the authentication counter (COMPTB) by a random rate.

10. The authentication method according to any one of Claims 1 to 8, characterized in that, in response to an authentication request, step b) consists of sending, at the authentication entity side (B), in addition to the authentication counter value (CB), a random value associated with said counter value (CB), said random value being different for each of the authentication counter values sent, each step of counter signature carried out during said method

being replaced by a signature step of the authentication counter value/associated random value couple, consisting of application of the cryptographic function (S) further comprising said associated random value as operand.

11. The authentication method according to any one of the preceding claims, characterized in that step c) consists in addition of verifying that the difference between the received authentication counter value (CB) and the stored counter value (CA) by the client entity is less than or equal to a predetermined value.

12. The authentication method according to any one of Claims 1 to 10, characterized in that with step c) not being verified, the following intermediate steps are implemented consisting of:

- sending the counter value (CA) stored by the client entity from the client entity (A) to the authentication entity (B);
- sending a temporary authentication counter value greater than said counter value (CA) stored by the client entity from the authentication entity (B) to the client entity (A), then:
- implementing steps d) to g) on the basis of the temporary authentication counter value and, in the case of success of authentication of said client entity,
- updating the authentication counter value (CB) corresponding to the current state of the counter (COMPTB) of the authentication entity (B) with the temporary authentication counter value and executing step h).

13. The authentication method according to any one of the preceding claims, characterized in that stage e) consists of transmitting the authentication counter value (CB) in addition to the authentication entity (B).

14. The authentication method according to any one of the preceding claims, characterized in that the authentication counter value (CB) is coded on at least 128 bits.

15. A chip card, characterized in that it comprises an integrated circuit and means for storing a secret key (K_A) and executing the method according to any one of Claims 1 to 14.

16. The chip card according to Claim 15, characterized in that it is a contactless chip card.

17. An authentication entity (B) of at least one client entity (A), characterized in that it comprises a chip card reader equipped with means for executing the method according to any one of Claims 1 to 14.

18. The authentication entity according to Claim 17, characterised in that it comprises a contactless chip card reader.